IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex Parte Hoffman et al.

Application for Patent: 09/587,092

Filed: May 31, 2000

Group Art Unit: 3693

Examiner: Borlinghaus, Jason M.

For:

SMART CARD TRANSACTIONS USING WIRELESS TELECOMMUNICATIONS NETWORK

APPEAL BRIEF

BEYER LAW GROUP LLP
P.O. Box 1687
Cupertino, CA 95015-1687
Attorneys for Appellant

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is Visa International Service Association, a subsidiary of Visa Inc.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

3. STATUS OF CLAIMS

The following claims have been rejected and appealed: claims 1, 4, 5, 7-9, 11, 12, 14, 15 and 23-25.

The following claims have been cancelled: 2, 3, 6, 10, 13 and 16-22.

The claims on appeal are reproduced below in the Appendix.

4. STATUS OF AMENDMENTS

No amendments were filed subsequent to final rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Systems and methods of the present invention allow value to be loaded onto a smart card within a mobile telephone handset using a wireless telecommunications network. The prior art previously restricted smart card loading at fixed terminals. Using the wireless telecommunications network, the handset becomes a remote terminal load device for the smart card.

5.1. Independent Claim 1

Claim 1 requires a smart card loading system (Figure 4, 200). The system includes a smart card 18, a mobile telephone handset 102 connected to a

telecommunication network (202, 104), a gateway computer 106, a funds issuer computer 204, and an authentication computer 206.

A subscriber identification module, smart card reader and smart card are inside the mobile telephone handset; an interface (such as a keypad and display) allows a user to indicate what value should be loaded onto the smart card (page 10, lines 12-15). The handset is able to generate a request message to load value onto the smart card (Figure 5A generally, 306, 330, 332, 334; page 13, lines 26-31). The handset also receives a response message to load value onto the smart card (Figure 5B generally, 336, 338, 340; page 14, lines 13-16).

The response message is implemented as an alphanumeric message integrated within an SMS message, and serves as a command input to the smart card in order to control operation of the smart card. (Page 5, lines 6-12; page 9, lines 18-30; page 10, lines 12-18).

The gateway computer receives the request message from the handset and retransmits the request message (330, 332, 334). The gateway computer also receives the response message and retransmits the response message to the handset (356, 358, 340). The funds issuer computer receives the request message and debits the consumer account (332; page 14, lines 3-6 and 29-31). The authentication computer is arranged to receive the request message (334), authenticate the smart card (page 14, lines 10-12), and generate the response message to the gateway computer (358).

The system thus authorizes the smart card in the mobile telephone handset to load value (page 14, lines 16-17).

5.2. Independent Claim 5

Claim 5 requires a smart card loading system (Figure 4, 200). The system includes a smart card 18, a mobile telephone handset 102 connected to a telecommunication network (202, 104), a gateway computer 106, and a funds issuer computer 204. The smart card is arranged to validate cryptographic certificates (page 8, lines 18-22; page 13, lines 4-25).

A subscriber identification module, smart card reader and smart card are inside the mobile telephone handset; an interface (such as a keypad and display)

allows a user to indicate what value should be loaded onto the smart card (page 10, lines 12-15). The handset is able to generate a funds request message to load value onto the smart card (Figure 5A generally, 306, 330, 332, 334; page 13, lines 26-31). The request message includes an authorization request certificate (page 13, line 26-page 14, line 12). The handset also receives an authentication response certificate in order to load value onto the smart card (Figure 5B generally, 336, 338, 340; page 14, lines 13-17).

The gateway computer receives the funds request message from the handset and retransmits the funds request message (330, 332, 334). The gateway computer also receives the authentication response certificate and retransmits the authentication response certificate to the handset (356, 358, 340).

The funds issuer computer receives the funds request message (332; page 14, lines 3-6 and 29-31), authenticates the smart card using the authorization request certificate (page 13, line 26-page 14, line 12; page 15, lines 24-26), and generates an authentication response certificate for delivery to the smart card via the gateway computer (page 14, lines 10-15; page 15, lines 24-26).

The smart card thus validates the authorization response certificate received via the mobile telephone handset and loads value (page 14, lines 16-17).

Note: the final action at page 7 seems to indicate that claim 5 includes a limitation of removing the smart card from the handset in order to interface with a point-of-sale terminal. Applicant believes that this limitation was removed in the reply filed March 1, 2006.

5.3. Dependent claim 7

Claim 7 requires that the authentication response certificate is implemented as an alphanumeric message integrated within an SMS message, and serves as a command input to the smart card in order to control operation of the smart card. (Page 5, lines 6-12; page 9, lines 18-30; page 10, lines 12-18).

5.4. Independent Claim 9

Claim 9 requires a method of loading value over a wireless telecommunications network onto a smart card (Figures 5A and 5B, 300).

A mobile telephone handset having a SIM receives a request from a user to load value onto the smart card (306). The handset generates a funds request message (page 12, line 21-page 13, line 25), and then sends this funds request message over the telecommunications network to a funds issuer computer (330, 332). The funds issuer computer is arranged to debit a user's account (page 11, lines 1-6).

A load request message is generated that includes a first cryptographic signature (page 13, lines 8-25). The load request message is sent over the telecommunications network to an authentication computer (330, 334); the authentication computer is arranged to authenticate the smart card (page 14, lines 10-12).

The handset receives a response message including a second cryptographic signature and an approval to load (340). The second cryptographic signature is validated and value is loaded onto the smart card (page 14, lines 15-17).

5.5. Dependent claim 11

Claim 11 requires that the response message is implemented as an alphanumeric message integrated within an SMS message, and serves as a command input to the smart card in order to control operation of the smart card. (Page 5, lines 6-12; page 9, lines 18-30; page 10, lines 12-18).

5.6. Independent Claim 12

Claim 12 requires a method of loading value over a wireless telecommunications network onto a smart card (Figures 5A and 5B, 300).

A mobile telephone handset having a SIM receives a request from a user to load value into a stored value application of the smart card (306; page 12, lines 17-26). A second application on the smart card capable of funding the stored value

application is opened (page 7, lines 28-30; page 12, lines 16-26; page 15, lines 5-14 and 18-20). The handset generates a funds request message including an authorization certificate (page 12, line 21-page 13, line 25; page 13, line 26-page 14, line 12), and then sends this funds request message over the telecommunications network to a funds issuer computer (330, 332). The funds issuer computer is arranged to authenticate the second application (page 15, lines 24-25), and to generate an authentication response certificate (page 14, lines 10-15; page 15, lines 24-26).

The smart card of the handset receives a response message including the authentication response certificate (340; page 15, lines 25-30). The authentication response certificate is validated (page 15, lines 30-31) and value is loaded onto the stored value application from the second application (page 14, lines 15-17; page 15, lines 11-14 and 31-32).

5.7. Dependent claim 14

Claim 14 requires that the response message is implemented as an alphanumeric message integrated within an SMS message, and serves as a command input to the smart card in order to control operation of the smart card. (Page 5, lines 6-12; page 9, lines 18-30; page 10, lines 12-18).

6. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 4-5, 7-9, 11-12, 14-15 and 23-25 are rejected under 35 USC §103 as being unpatentable over *Rankl*, *Manterfield* and Admissions.

7. ARGUMENT

7.1. Claims 1, 5, 9 and 12: No references disclose a mobile telephone having both a smart card and a subscriber identification module (SIM).

Claim 1 requires "a mobile telephone handset in communication with said telecommunications network, said handset including a subscriber identification

module (SIM) that is separate from said smart card and functions to allow a user to access said telecommunications network" (emphasis added). Claim 5 also requires a handset having a SIM that is separate from the smart card. Claims 9 and 12 also both require receiving a request at a mobile telephone handset having a SIM to load value onto a smart card. The SIM is separate from the smart card.

None of the cited references disclose a mobile telephone handset that has both a SIM and a smart card, and the final action does not allege that any reference discloses a handset having both a SIM and a smart card. On this basis alone, it is respectfully requested that the rejection of independent claims 1, 5, 9 and 12 be withdrawn.

The Mondex system described at pages 343-345 of *Rankl* discloses a conventional telephone with a built-in smart card reader, but there is no discussion of a separate SIM. The inter-sector (IEP) electronic purse described at pages 336-337 of *Rankl* discloses a smart card, but there is no discussion of a mobile telephone, let alone a smart card and a SIM in a mobile telephone. The GSM Network at pages 362-364 of *Rankl* at Figure 13.2 shows a mobile telephone having a SIM, but there is no disclosure of an additional smart card within the mobile telephone.

The final action on page 5, third paragraph, alleges that the SIM of Figure 13.2 "is separate from said smart card." This implicit allegation that an additional smart card is somewhere present in Figure 13.2 is not accurate. Figure 13 .2 shows a single SIM within a mobile telephone; there is no additional, separate smart card present as required by independent claims 1, 5, 9 and 12. For this reason, it is respectfully requested that the rejection be withdrawn.

7.2. Claims 1, 5, 9 and 12: It is not obvious to combine the three separate smart card technologies of *Rankl.*

The final action has rejected independent claims 1, 5, 9 and 12 primarily on the basis of combining three separate smart card technologies from *Rankl.* (Claim 1 is rejected in detail; claim 5 "is therefore rejected using the same art and rationale as

applied in the rejection of claims 1 and 4;" and claims 9 and 12 "are therefore rejected using the same art and rationale as previously utilized.") Applicant disagrees with the basic premise of the final action, namely, that it would be obvious to simply combine these three separate smart card technologies in order to arrive at the invention of claims 1, 5, 9 and 12.

The final action uses as a base reference the Mondex system described at pages 343-345 of *Rankl*. The Mondex system shows a conventional, wired telephone in Figure 12.15 and describes that the telephone has a built-in smart card reader and that loading of the smart card occurs over the telephone. "It allows money to be transferred over the line during the call," (page 344, second paragraph, underline added). In other words, a transfer occurs over the wired telephone line; this is not a wireless telephone. The Mondex system does not show a mobile telephone incorporating a SIM (subscriber identification module) into which an inserted smart card is loaded as required by claim 1. Claim 1 requires both a SIM and a smart card. Figure 12.15 only shows a conventional, fixed, wired telephone; the background of the present application points out that fixed loading terminals (such as a wired telephone, terminal or computer) are less than desirable. Application of the Mondex system to a wireless, mobile telephone having both a SIM and a smart card is clearly not contemplated.

As a second reference, the final action refers to the inter-sector (IEP) electronic purse described at pages 336-337 of *Rankl*. This section describes loading a smart card at a fixed terminal, but does not describe loading a smart card while the smart card is incorporated within a mobile telephone that also incorporates a SIM. The paragraphs on page 337 simply describe loading an electronic purse at a fixed, physical terminal. There is no discussion of any applicability to a wireless, mobile telephone that also includes a SIM, as required by claim 1.

For the third reference, the final action refers to the GSM Network at pages 362-364 of *Rankl*. The GSM Network shows in Figure 13.2 a mobile telephone that incorporates a subscriber identification module (SIM). But, this mobile telephone does not incorporate a separate smart card onto which value can be loaded, in addition to including the SIM. In fact, there is no disclosure whatsoever concerning

loading value onto an additional smart card. The SIM is not arranged to receive value; its only purpose is to facilitate communication.

The final action at page 6, first and second full paragraphs, is unclear as to whether all three technologies are being combined to arrive at the present invention, or whether the Mondex system is being modified by the other two technologies separately in order to arrive at the present invention. In either case, Applicant respectfully asserts that inexcusable hindsight is being used to allege that it is obvious to combine these technologies to arrive at the present invention. Applicant assumes that all three technologies are being combined because only the third GSM network discloses a mobile telephone.

The final action suggests at page 6 that it would have been an obvious matter to modify the fixed, wired telephone of the Mondex system by incorporating the electronic purse technology and the GSM network to arrive at the present invention. Applicant disagrees. Mondex simply shows the prior art which is a fixed, wired telephone into which a smart card may be inserted in order to transfer value. The electronic purse only describes a prior art purchase and load using a fixed terminal and a single smart card. Neither these disclose a mobile telephone nor a second, separate SIM.

The third reference, the GSM network, does show a mobile telephone, but only a single SIM is shown; there is no additional, separate smart card. Simply saying that three references should be combined does not mean that they can be combined, and does not magically disclose a mobile telephone having both a SIM and a separate smart card. There would have been no motivation to include both a SIM and a smart card in a mobile telephone. One of skill in the art will appreciate that there are technical details and nonobvious problems to overcome.

It is not reasonable to simply assume that one of skill the art would look at the fixed loading systems of Mondex and the electronic purse, understand that a wireless GSM telephone exists, and suddenly arrive at the present invention. *Rankl* does not disclose any details or means by which value may be loaded onto a smart card in a wireless telephone over a wireless telecommunications network. Absent these details (such as use of cryptography, messages passed to and from a mobile telephone, both a

SIM and a smart card within a mobile telephone), it cannot be assumed that one of skill in the art would have arrived at the present invention. Because none of these details are present in the cited references, Applicant submits it is not simply an obvious matter to combine all three references and arrive at the present invention. For at least this reason, it is requested that the §103 rejection of independent claims 1, 5, 9 and 12 be withdrawn.

7.3. Claims 1, 7, 11 and 14: It is not obvious to use an SMS text message to control a smart card.

Independent claim 1 and dependent claims 7, 11 and 14 require that a response message or response certificate is implemented as an alphanumeric message integrated within a standard SMS message, and that this alphanumeric message is used to control operation of the smart card in the mobile handset. The final action at pages 9-11 states that this limitation would have been obvious. Applicant disagrees.

A response to control the smart card is cleverly inserted into an SMS message so that it may be transmitted over a wireless telecommunications network to the mobile telephone and thence to the smart card attached. This feature is neither taught nor suggested by any of the cited references. Applicant acknowledges that the *Manterfield* reference discloses that SMS messages are alphanumeric messages. Applicant agrees that SMS messages were existing at the time of the present invention; but Applicant is not simply claiming sending a generic nonfunctional text message or data using SMS. The above claims very specific specifically point out that commands intended for the smart card are implemented as an alphanumeric message and are integrated within a standard SMS message. The alphanumeric message transmits important commands and security data (such as cryptographic certificates) to a smart card. SMS is not being used to simply send a text message; it is being used to control operation of a smart card within a mobile telephone.

Applicant agrees that SMS was known in the art to send text messages from one person to another person; *i.e.*, the message is intended for a human to read. There is no disclosure in any reference of using SMS messages (which contain human-readable words) to actually be destined for a microprocessor in a mobile telephone to be interpreted by that microprocessor. Applicant asserts that while SMS was known

at the time to send a text message to a human, it would not have been obvious to think of sending a response message not intended for a human, but intended for a microprocessor instead. Because SMS was designed to send messages to people, one of skill in the art would not have made the mental leap to think of using SMS to send a message to a microprocessor in a mobile telephone.

While it might have been obvious at the time of the invention to send an alphanumeric SMS text message to a teenager saying "HOW R U," it would not have been obvious to send an alphanumeric SMS message to a smart card in a mobile telephone that is not only unintelligible to a human, but also that is able to control the smart card.

7.4. Claim 12: Funding a stored value application using a second application on the smart card is not taught or suggested in the art of record.

Claim 12 requires as a second step "opening a second application on said smart card capable of funding said stored value application," and as a seventh step, "loading said value onto said stored value application of said smart card from said second application." Claim 12 differs from the other independent claims in that value is loaded onto the smart card from a second application on the smart card itself, rather than from a source outside the smart card. Such an embodiment is described on page 15.

The final action does not allege that these two steps are present in any of the cited references. For this reason alone, it is respectfully requested that the rejection of claim 12 be withdrawn.

There is no disclosure in the Mondex system of a second application on the smart card loading value into a stored value application on a smart card. In fact, Figure 12.15 of *Rankl* shows that funds are received from outside the card from a wallet or from another smart card. Likewise, the electronic purse of *Rankl* only discloses that the purse is loaded from an external security module in an associated physical terminal. The GSM Network of *Rankl* does not have any discussion of

loading value onto a smart card in a mobile telephone, let alone opening a second application for that purpose.

8. CONCLUSION

In view of the foregoing, it is respectfully submitted that the above rejection is erroneous and it is requested that this rejection be reversed.

Respectfully submitted,
BEYER LAW GROUP LLP

/Jonathan O. Scott/

Jonathan O. Scott
Registration No. 39,364

BEYER LAW GROUP LLP
Attorneys for Appellant

9. CLAIMS APPENDIX LISTING CLAIMS ON APPEAL

1. A smart card loading system for loading value over a wireless telecommunications network onto a smart card, said smart card loading system comprising:

a smart card;

a mobile telephone handset in communication with said telecommunications network, said handset including a subscriber identification module (SIM) that is separate from said smart card and functions to allow a user to access said telecommunications network, a smart card reader for communicating with said smart card when said smart card is inserted in said handset, and an input interface for indicating a value to be loaded onto said smart card, said handset being arranged to generate a request message to load said value onto said smart card and to receive a response message to load said value onto said smart card, wherein said response message is implemented as an alphanumeric message integrated within a Short Message Service (SMS) message of said telecommunications network, said alphanumeric message serving as a command input to said smart card used to control operation of said smart card;

a gateway computer arranged to receive said request message from said handset over said telecommunications network and to retransmit said request message, said gateway computer being further arranged to receive said response message and to retransmit said response message to said handset;

a funds issuer computer arranged to receive said request message and to debit a consumer account associated with said smart card; and

an authentication computer arranged to receive said request message and to authenticate said smart card, said authentication computer being further arranged to generate said response message for transmission to said gateway computer, whereby said smart card is authorized to load said value via said handset.

4. A smart card loading system as recited in claim 1 wherein said authentication computer authenticates said smart card using a first cryptographic signature and

generates a second cryptographic signature to authenticate a load response, whereby said transaction is secured.

5. A smart card loading system for loading value over a wireless telecommunications network onto a smart card, said smart card loading system comprising:

a smart card arranged to validate cryptographic certificates;

a mobile telephone handset in communication with said telecommunications network and arranged to accept said smart card, said handset including a subscriber identification module (SIM) that is separate from said smart card and functions to allow a user to access said telecommunications network, a smart card reader for communicating with said smart card when said smart card is inserted in said handset, and an input interface for indicating a value to be loaded onto said smart card, said handset being arranged to generate a funds request message which includes an authorization request certificate and being arranged to receive an authentication response certificate in order to load said value onto said smart card;

a gateway computer arranged to receive said funds request message from said handset over said telecommunications network and to retransmit said funds request message, said gateway computer being further arranged to receive said authentication response certificate and to retransmit said authentication response certificate to said handset;

a funds issuer computer arranged to receive said funds request message, to authenticate said smart card using said authorization request certificate, and to generate an authentication response certificate for delivery to said smart card via said gateway computer, whereby said smart card validates said authorization response certificate received via said mobile telephone handset and loads said value.

7. A smart card loading system as recited in claim 5 wherein said authentication response certificate is implemented as an alphanumeric message integrated within a Short Message Service (SMS) message of said telecommunications network, said alphanumeric message serving as a command input to said smart card used to control operation of said smart card.

8. A smart card loading system as recited in claim 5 wherein in response to a successful load, said handset is arranged to generate a transaction certificate to be used for irrepudiation.

9. A method of loading value over a wireless telecommunications network onto a smart card, said method comprising:

receiving at a mobile telephone handset with a subscriber identification module a request from a user to load a value onto said smart card inserted in said handset;

generating a funds request message which includes said value;

sending said funds request message over said telecommunications network to a funds issuer computer arranged to debit an account associated with said user;

generating a load request message including a first cryptographic signature;

sending said load request message over said telecommunications network to an authentication computer arranged to authenticate said smart card;

receiving a response message which includes a second cryptographic signature and an approval to load; and

validating said second cryptographic signature; and

loading said value onto said smart card.

11. A method as recited in claim 9 wherein said response message is implemented as an alphanumeric message integrated within a Short Message Service (SMS) message of said telecommunications network, said alphanumeric message serving as a command input to said smart card used to control operation of said smart card.

12. A method of loading value over a wireless telecommunications network onto a smart card, said method comprising:

receiving at a mobile telephone handset with a subscriber identification module a request from a user to load a value into a stored-value application of said smart card inserted in said handset;

opening a second application on said smart card capable of funding said stored-value application;

generating a funds request message which includes said value and an authorization certificate;

sending said funds request message over said telecommunications network to a funds issuer computer arranged to authenticate said second application and to generate an authentication response certificate;

receiving through the mobile telephone handset to the smart card a response message which includes said authentication response certificate;

validating said authentication response certificate; and

loading said value onto said stored-value application of said smart card from said second application.

14. A method as recited in claim 12 wherein said response message is implemented as an alphanumeric message integrated within an Short Message Service (SMS) message of said telecommunications network, said alphanumeric message serving as a command input to said smart card used to control operation of said smart card.

15. A method as recited in claim 12 further comprising:

generating a transaction certificate to be used for irrepudiation.

23. A smart card loading system as recited in claim 1 wherein said response message generated remotely from said mobile telephone handset and intended for

said smart card is implemented as an alphanumeric message and is integrated within an SMS message of said telecommunications network, said alphanumeric message serving as a command input to said smart card used to control operation of said smart card.

24. A method as recited in claim 9 further comprising:

removing said smart card from said handset;

placing said removed smart card into association with a smart card reader; and

using said smart card reader to debit said smart card to perform a purchase.

25. A method as recited in claim 12 further comprising:

removing said smart card from said handset;

placing said removed smart card into association with a smart card reader; and

using said smart card reader to debit said smart card to perform a purchase.

10. EVIDENCE APPENDIX

No evidence has been submitted pursuant to §§ 1.130, 1.131, or 1.132 of 37 CFR, nor has any other evidence been entered by the examiner.

11. RELATED PROCEEDINGS APPENDIX

There have been no decisions rendered by a court or the Board in any related proceeding.